AD-HOC RADIO COMMUNICATION VERIFICATION SYSTEM

Abstract

An aspect of the present invention is to easily verify data integrity in data transmission and reception by means of an ad-hoc radio connection. A requester and requested end of an establishment of a cipher communication path are defined as source A and destination B, respectively. A predetermined verification data generation algorithm ID1 is arranged in advance between source A and destination B. Source A sends its own public key Kp to destination B, and at the same time generates verification data Xp based on Kp using ID1 and outputs Xp to its own verification image display section. On the other hand, destination B receives data Kx that is transmitted from source A as Kp, then generates verification data Xx based on Kx using ID1 and outputs Xx to its own verification image display section. A verifier determines that data integrity is secured if Xp and Xx displayed in the verification image display sections of source A and destination B match.

[Selected Drawing] Fig. 4